

Identity Theft Task Force

Submission of Public Comments

Section I (Maintaining Security of Consumer Data), Part 1 (Government Use of SSNs):

Addressing the Task Force's Interim Recommendations on data protection in the public sector, I provide the following comment:

PROBLEM: The Department of Defense, in which I am a commissioned officer in the US Army, uses the Social Security Number (SSN) as the Military Identification Number for all uniformed military. Further, it also uses the SSN as the identification number for all dependents of uniformed military members, under the DEERS system. The Department of Defense at one time issued a "Serial Number" to its servicemembers, but shifted to the universal use of Social Security Numbers several decades ago. The Geneva Conventions merely require an identifying number of some sort, but obviously do not mandate use of a Social Security Number.

EXTENT OF PROBLEM: Nearly all documents in the military, from counseling statements and evaluations to traffic tickets, military driver's licenses, training records, awards, and pay records, use the SSN as the identification number for the military. Similarly, the DEERS system requires the military sponsor's SSN on nearly all documents concerning his or her dependents, such as medical and educational records. The US Army Morale Welfare and Recreation program even requires enrollment of family members and dependent children into a database (called InfoTrac or RecTrac) using both their and their sponsor's SSN in order to obtain childcare services or use fitness centers and recreation facilities.

IMPACT: The Department of Defense (along with the Department of Veterans' Affairs) has a poor track record in protecting servicemembers from identity theft as a consequence of this policy. Stolen laptops and breached databases have made news in the past several years. Recently, I was notified by a DOD healthcare contractor not even based in the US, International SOS (which handles healthcare for families overseas), that an employee laptop was stolen in London containing my name and SSN. However, in this case and other cases, DOD does not comport with the industry standard of at least providing credit monitoring protection for free after their negligence in losing my data.

RECOMMENDATIONS: (1) Require DOD to find an alternative to the SSN as means of identification. In a response to my Congressman on this issue generated by my correspondence with him, the DOD POC stated that it would be too expensive and simply not worth doing because identity thieves would quickly have any new number stolen. The DOD POC missed the point that the new number would not be useful in stealing a servicemember's identity for financial crimes (the primary reason), because the new number would not be used by any financial institution for their purposes. Alternative (A) would be to generate a unique military serial number for all servicemembers (as in the past), and their dependents would have an extension of that number. Alternative (B) would be to use our Selective Service numbers, which all males in the military possess

and which is different than our SSNs; female servicemembers could be assigned comparable numbers.

(2) Impose a financial penalty on DOD in the form of mandatory payment of credit monitoring services for each servicemember for any instance of SSNs in DOD possession being lost or stolen. DOD would soon recognize that the costs of repeated payments for credit monitoring services could be prevented by switching to a non-SSN identifying number.